AMENDMENTS TO THE SPECIFICATION

Please delete the section entitled "SUMMARY OF THE INVENTION" in its entirety and substitute the following section therefor:

SUMMARY OF THE INVENTION

[0021] The present invention, among other applications, is directed to solving these and other problems and disadvantages of the prior art. The present invention provides a superior technique for performing cryptographic operations within a microprocessor. In one embodiment, an apparatus for performing cryptographic operations is provided. The apparatus has an x86-compatible microprocessor that includes fetch logic, algorithm logic, and execution logic. The fetch logic is configured to receive a single, atomic cryptographic instruction, wherein the single, atomic cryptographic instruction is one of the instructions in an application program. The application program is executed by the x86-compatible microprocessor. The single, atomic cryptographic instruction prescribes ~~one of the cryptographic operations~~an encryption operation and one of a plurality of cryptographic algorithms. The algorithm logic is operatively coupled to the single, atomic cryptographic instruction. The algorithm logic directs the x86-compatible microprocessor to execute the encryption operation ~~one of the cryptographic operations~~ according to the one of a plurality of cryptographic algorithms. The execution logic is operatively coupled to the algorithm logic. The execution logic executes the encryption operation~~one of the cryptographic operations~~. The execution logic includes a cryptography unit for executing a plurality of cryptographic rounds required to complete the encryption operation~~one of the cryptographic operations~~.

[0022] One aspect of the present invention contemplates an apparatus for performing cryptographic operations. The apparatus has an x86-compatible microprocessor that includes a cryptography unit and algorithm logic. The cryptography unit executes ~~one of the cryptographic operations~~a decryption operation responsive to receipt of a single, atomic cryptographic instruction that prescribes the decryption operation~~one of the cryptographic operations~~, where the single, atomic cryptographic instruction is one of the instructions in an application program that are fetched from memory by fetch logic in the x86-compatible microprocessor, and wherein the x86-compatible microprocessor executes the application program. The single, atomic cryptographic instruction has an algorithm field that prescribes one of a plurality of cryptographic algorithms to be employed when executing the decryption operation~~one of the cryptographic operations~~. The algorithm logic is operatively coupled to the cryptography unit. The algorithm logic directs the x86-compatible microprocessor to perform the decryption operation~~one of the cryptographic operations~~ according to the one of the plurality of cryptographic algorithms.

[0023] Another aspect of the present invention provides a method for performing cryptographic operations in a device. The method includes fetching a single, atomic cryptographic instruction for execution by an x86-compatible microprocessor, where the single, atomic cryptographic instruction prescribes ~~one of a plurality of cryptographic operations~~an encryption operation and one of a plurality of cryptographic algorithms; and, via a cryptography unit in the x86-compatible microprocessor, executing the ~~one of the cryptographic operations~~encryption operation according to the one of the cryptographic algorithms.